CHAPTER SEVEN

TAKING ADVANTAGE OF CYBERSPACE WITHOUT BECOMING VULNERABLE

Chapter 7 - Taking Advantage of Cyberspace Without Becoming Vulnerable

Background

The Department of Defense vision is to achieve information superiority through global, affordable, and timely access to reliable and secure information for worldwide decisionmaking and operations. In support of this vision, the DoD has as its mission to provide, in a secure fashion, the right information, at the right place and time from the right sources, in a form that users can understand and reliably use to accomplish their missions and tasks. Information Assurance (IA) is essential to achieve and maintain information superiority. IA is integral to the ability to integrate intelligence, command-and-control, and battlefield awareness functions into joint and combined operations. IA is an essential element for implementing protection of critical national infrastructures mandated by the Presidential Decision Directive #63, Critical Infrastructure Protection.

Initiatives

In order to simplify, streamline, and save resources, the DoD uses electronic commerce to enable easy exchange of information and a rapid response to warfighter needs. However, operating in this environment creates vulnerabilities that must be addressed to ensure the safeguarding of the information and the associated infrastructure that constitute the Defense Information Infrastructure.

Chapter Seven comprises the following initiatives:

7.01 Information Technology
7.02 Electronic Environment - Characteristics & Challenges
7.03 Information Assurance
7.04 DoD's Information Assurance Strategy
7.05 Critical Infrastructure Protection

The team's primary focus for this project was 7.03 Information Assurance. This initiative enables the DoD to address the vulnerabilities inherent in a distributed, highly connected, network environment.

Chapter 7 - Taking Advantage of Cyberspace Without Becoming Vulnerable

- **Background**
  - Achieve information superiority through Information Assurance (IA)
  - IA is an essential element for carrying out PDD #63, Critical Infrastructure Protection
- **Initiatives**
  - Information Technology
  - Electronic Environment - Characteristics & Challenges
  - Information Assurance
  - DoD’s Information Assurance Strategy
  - Critical Infrastructure Protection

Chapter 7 - Taking Advantage of Cyberspace Without Becoming Vulnerable

Performance Measures

Discussion of performance measures is contained in the Performance Measures section under Initiative 7.03

Recommendations

It is critical that DoD's vital information resources are secure and protected. Initiatives such as Information Assurance needs to be integrated into all facets of military operations. This integration involves more than simply acquiring technology. It requires improving the awareness of individuals throughout the Department of the criticality of information operations and the role of IA in support of operational missions. Most important, it requires a clear operational understanding of the risks and impacts of an inadequate IA posture on defense missions. Therefore, it is recommended that IA awareness be an ongoing activity, with review of strategies and improvement opportunities throughout the Department.

Chapter 7 - Taking Advantage of Cyberspace Without Becoming Vulnerable

- **Performance Measures**
  - Discussed under Initiative 7.03
- **Recommendation**
  - IA has a pervasive impact on the DoD vision and mission; therefore, review and seek improvement opportunities for IA awareness

Initiative 7.03 - Information Assurance

Background

The Director of Infrastructure and Information Assurance, Office of the Deputy Assistant Secretary of Defense (Security and Information Operations) is cognizant of the training of personnel to increase their IA awareness and capabilities. Security Training and Certification is a key component of the DoD's Information Management (IM) Strategy. One of the most important components of a security strategy is a control procedure to help restrict unauthorized access, yet it is one of the least implemented procedures. Another key component in the IM Strategy is the issuing of digital certificates to the entire DoD user population to raise the overall level of IA consistent with operational requirements. Fundamentally, the linchpin to allow IA capabilities to address the pervasiveness of information throughout warfighting and business operations is the ability to ensure the validity of the electronic data. The DoD PKI provides a solid foundation for IA capabilities across the Department. Basically, five security principles can be applied to electronic transactions. Although each focuses on securing a distinct aspect of a transaction, all five must work in concert to provide a truly secure electronic application. The utilization of at least a medium assurance certificate ensures these five principles:

- Authentication ensures that both parties are who they say they are.
- Privacy protects confidential information by using various forms of cryptography.
- Authorization ensures that each party is allowed to enter the transaction.
- Integrity ensures that a transaction has not been altered or destroyed.
- Nonrepudiation provides evidence for both parties that the transaction actually occurred.

A third area addressed in this initiative is making IA a part of the DoD mission-readiness criteria. This is done by categorizing the mission functions and system elements of the infrastructure. Furthermore, once the systems have been categorized, they can undergo a certification and accreditation process to ensure compliance with mission, architecture, and security requirements. Increasing the IA operational capabilities is a fourth component of the IM Strategy. As no single solution exists that can provide the necessary protection, it is achieved through the application of the defense-in-depth concept (e.g., hardening the network infrastructure; protecting the enclave boundaries; implementing a common, integrated DoD PKI; etc.).

7.03 - Information Assurance

- **Background**
  - There are four components to the DoD strategy
    - Increase Information Assurance (IA) awareness
    - Increase level of IA
    - Integrate IA into mission readiness criteria
    - Increase IA operational capability

Initiative 7.03 - Information Assurance

Approach

The project team investigated all current publicly available information to augment their existing background expertise in security training and certification. Extensive interviews were then held with the initiative lead to gain a direct understanding of underlying goals and currently available information/data that could be used in developing performance measures and scorecards. Following data assessment and review of measures external to DRI, the team developed proposed performance measures and presented those to the initiative lead. Following acceptance of the new measures, scorecards were developed to aptly portray DoD performance.

Performance Measures

The fundamental goal for the Information Assurance Initiative is to ensure that the DoD's vital information resources are secure and protected. This is achieved, in large part, through making IA an integral part of personnel, operations, and technology. At this point, the most effective way to measure the progress of the IA rollout is to establish performance measures that identify the percentage of completion toward milestones for training, certification, assurance level, operational, and accreditation goals. Based on team evaluations and recommendations, the initiative lead agreed that incorporation of these metrics are an effective way to measure the IA presence within the DoD. The performance metrics measure:

- Extent of security training and certification
- Issuance of Class 3 (or higher) digital certificates
- Performance of IA readiness assessments
- Implementation of defense-in-depth concept
- DITSCAP compliance

7.03 - Information Assurance

- **Approach**
  - Review of available documentation
  - In-depth interviews with initiative lead
  - Joint development of metrics/scorecards
- **Performance Measures**
  - Extent of security training and certification,
  - Issuance of Class 3 (or higher) digital certificates,
  - Performance of IA readiness assessments,
  - Implementation of defense-in-depth concept
  - DITSCAP compliance

Initiative 7.03 - Information Assurance

Recommendations

It is recommended that the newly developed metrics be adopted by the DRI for use on this initiative. Their adoption will provide outcome metrics with which to assess the DoD's progress in protecting its vital information resources. In the future, it may be beneficial for the DoD to develop more specific or more refined metrics. For example, it would be beneficial to break down the certificate rollout into individual performance metrics (e.g., ID proofing, registration process, etc.) to provide greater visibility into the efficiency and effectiveness of the IA process. A balanced scorecard approach could assist in establishing a comprehensive set of new performance measures for future phases of this initiative.

7.03 - Information Assurance

- **Recommendations**
  - Adopt new metrics
    - Assess progress of IA rollout
    - Percentage of completed measurement
  - Once IA process is established, consider measures that examine process efficiency and effectiveness more closely. Use a balanced scorecard approach.

7.03 - Information Assurance

Goal: Train and certify DoD network managers, operators, system administrators, and all other personnel involved in the operation and management of the Global Information Grid (GIG) and its component systems by January 1, 2001.

Performance Measure: Percentage of personnel trained and certified

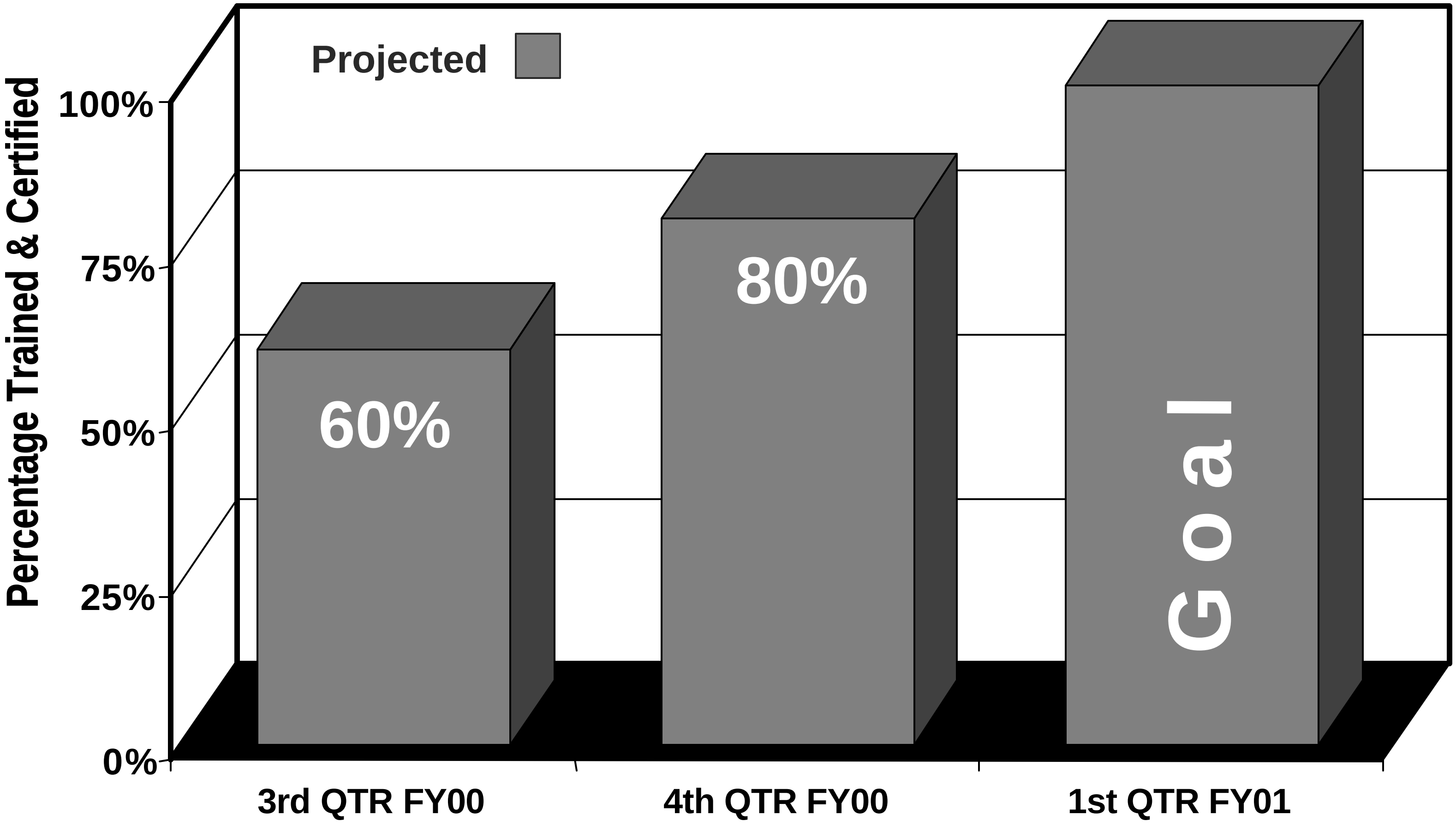
			Goal
	3rdQ FY 2000	**4thQ FY 2000**	**1stQ FY 2001**
Projected	**60%**	**80%**	**100%**

Source: DoD Information Assurance (IA) Policy Memorandum

Organization, Systems, and Other Issues: Even when the strongest logical controls exist, the probability of prohibiting unauthorized access is unlikely if the security awareness of company employees is low. This metric enables the DoD to assess the progress of its IA awareness training program. In addition, training and certification must extend into the contractor community supporting DoD.

Increase IA Awareness Through Secure Operations/Management Training and Certification

Percentage of Personnel Trained and Certified in Secure Operations/Management



7.03 - Information Assurance

Goal: Implement the DoD PKI consistent with the May 6, 1999 policy memorandum, DoD PKI road map, DoD PKI Implementation Plan, and the DoD PKI Certificate Policy

Performance Measure: Percentage of installations which have been issued Class 3 (or higher) digital certificates

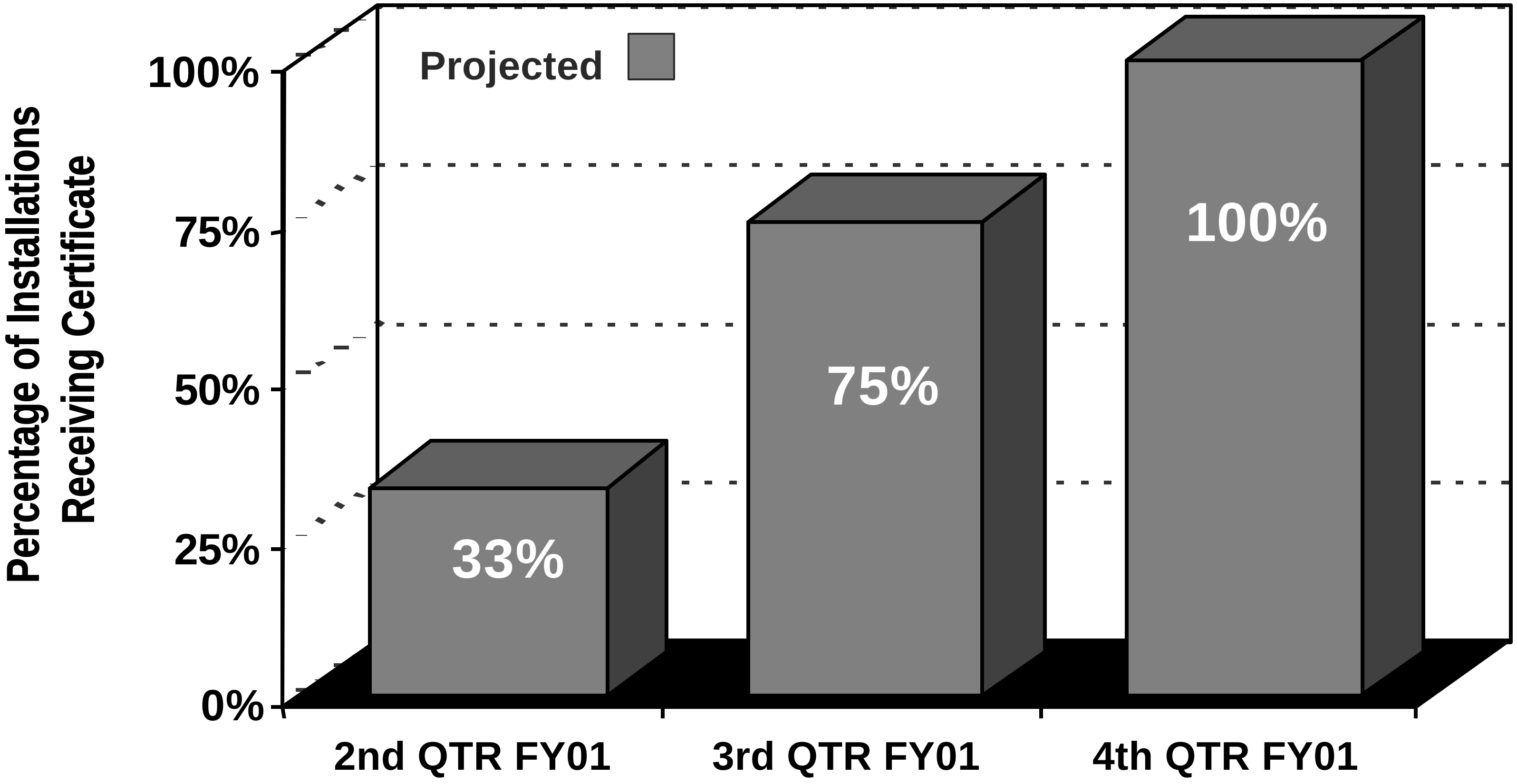
			Goal
	2ndQ FY 2001	**3rdQ FY 2001**	**4thQ FY 2001**
Projected	**33%**	**75%**	**100%**

Source: DoD Information Assurance (IA) Policy Memorandum

Organization, Systems, and Other Issues: The use of digital certificates to ensure the validity of electronic data raises the level of IA consistent with operational requirements. The goal is to issue to all DoD personnel Class 3 (minimum) certificates by October 1, 2001. Class 3 equals a medium assurance software token. By January 2002, the DoD will no longer issue Class 3 certificates. This metric allows the DoD to assess the progress of the PKI implementation.

Increase Level of Information Assurance Across Mission and Business Processes

Percentage of Installations Receiving Issuance of Class 3(or Higher) PKI Certificates



7.03 - Information Assurance

Goal: Designate all GIG functions as either mission-critical, mission-essential, or mission-support by April 1, 2001

Performance Measure: Percentage of mission functions and system elements assessed and categorized

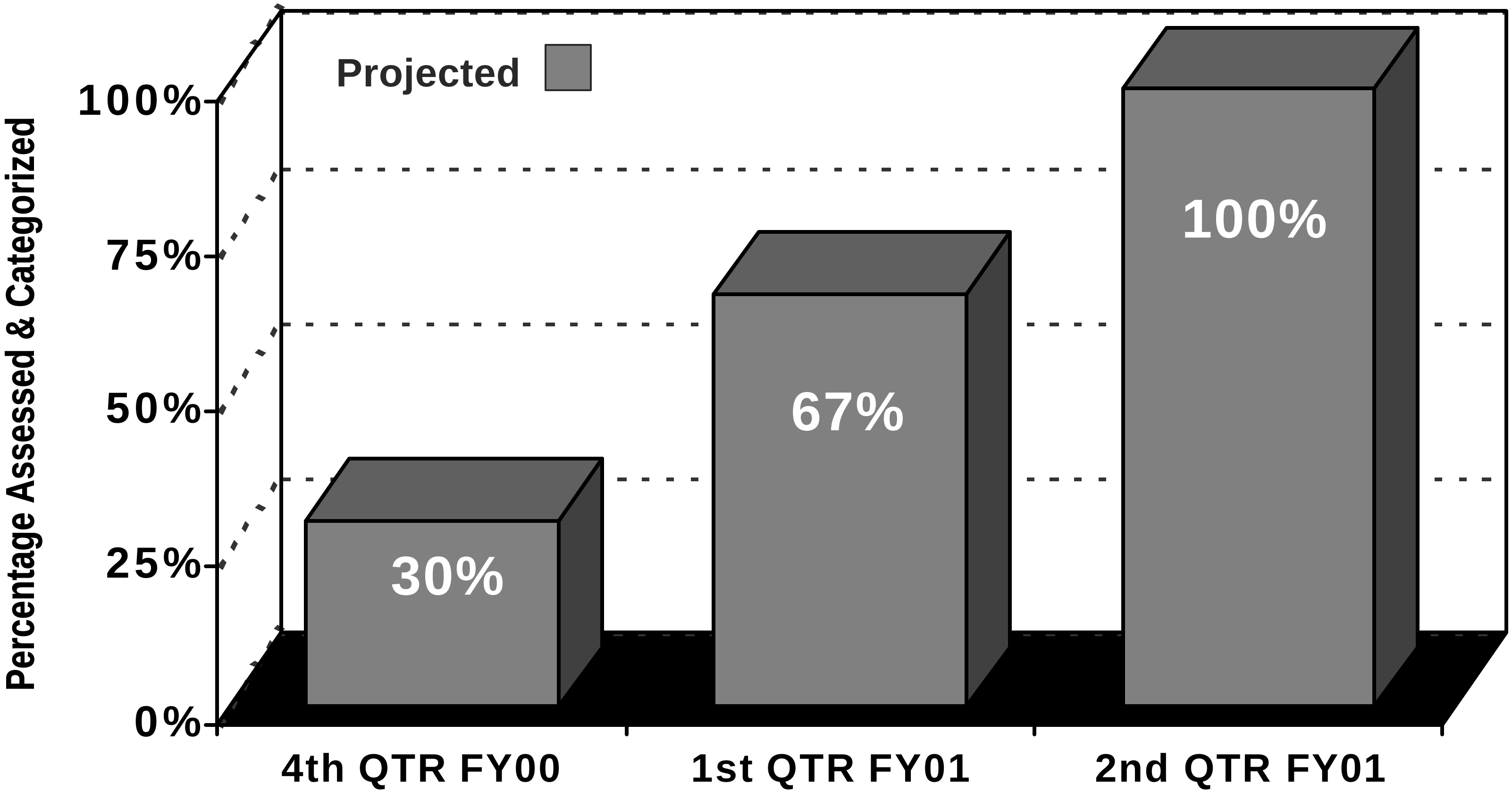
			Goal
	4thQ FY 2000	**1stQ FY 2001**	**2ndQ FY 2001**
Projected	**30%**	**67%**	**100%**

Source: DoD DIAP Strategic Objective

Organization, Systems, and Other Issues: Identifying and assessing information assurance readiness for mission functions and information system elements of the Global Information Grid (GIG) increases visibility of mission capabilities. Categorizing the resources allows the DoD to apply the appropriate security controls and IA technology. DoD infrastructure owners, in coordination with the Joint Staff and the Critical Asset Assurance Program, will perform the assessments. This metric enables the DoD to determine the progress of this activity.

Increase Visibility of Mission Capabilities Through Information Assurance Readiness Assessments

Percentage of Mission Functions and Systems Assessed and Categorized



7.03 - Information Assurance

Goal: Implement defense-in-depth concept across the GIG by April 1, 2002

Performance Measure: Percentage of the GIG with protection measures applied

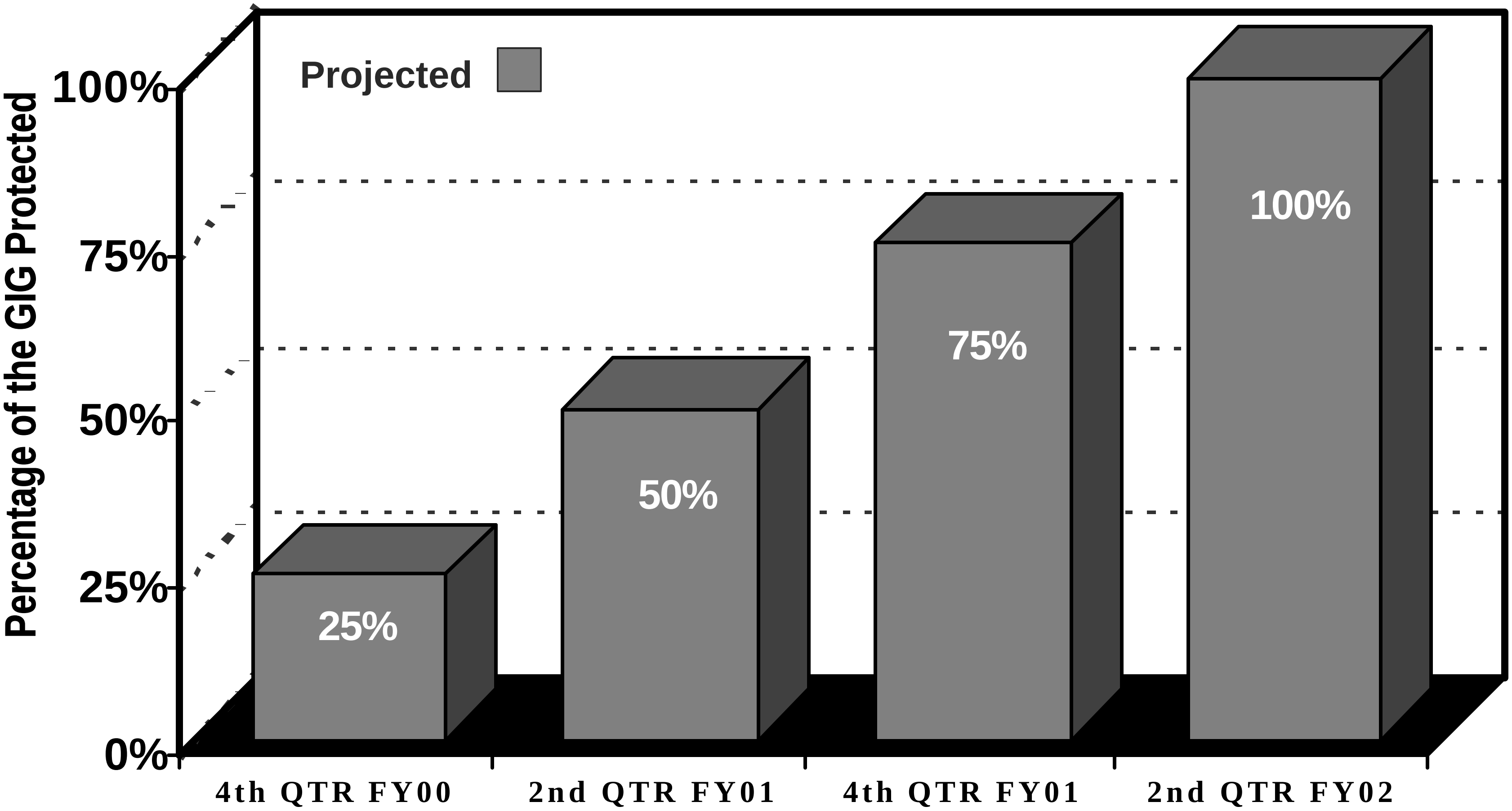
				Goal
	4thQ FY 2000	**2ndQ FY 2001**	**4thQ FY 2001**	**2ndQ FY 2002**
Projected	**25 %**	**50%**	**75%**	**100%**

Source: DoD DIAP Strategic Objective

Organization, Systems, and Other Issues: The defense-in-depth concept comprises layered defensive mechanisms and practices and is the only way to achieve the necessary level of IA in a highly distributed environment. It includes overlays of network systems, firewalls, architecture, routers, etc. This concept will be applied to each operating assurance level and shall be applied in accordance with DoD criteria. This metric allows the DoD to develop a schedule for, and assess the progress of, the application of the defense-in-depth concept across the GIG.

Increase Information Assurance Operational Capability Levels

Percentage of DoD Systems Deploying
Defense In-Depth Concept Across the Global Information Grid (GIG)



7.03 - Information Assurance

Goal: Complete certification and accreditation process IAW Defense Information Technology Security Certification and Accreditation Process (DITSCAP) on all GIG components by October 1, 2002

Performance Measure: Percentage of GIG components accredited

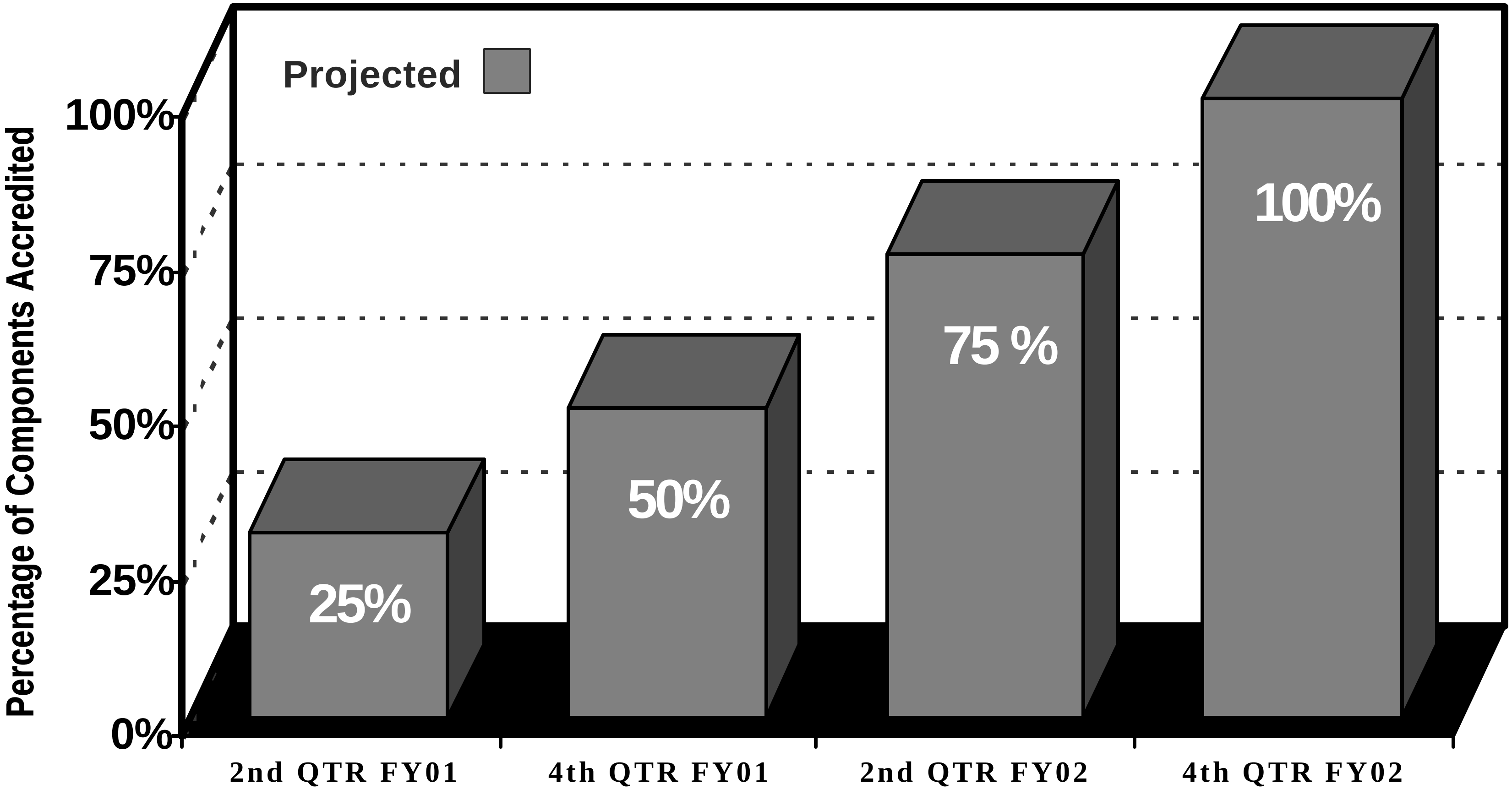
				Goal
	2ndQ FY 2001	**4thQ FY 2001**	**2ndQ FY 2002**	**4thQ FY 2002**
Projected	**25%**	**50%**	**75%**	**100%**

Source: DoD GIG IA Policy Memorandum

Organization, Systems, and Other Issues: DITSCAP-compliant certification and accreditation (C&A) are essential for ensuring that the appropriate security measures and IA technology are being applied to the components of the GIG. As GIG components are modified, recertification must be done on the resultant system, causing this process to continue beyond October 1, 2003. This metric allows the DoD to develop a schedule for, and assess the progress of, the C&A process.

Increase Information Assurance Levels by Ensuring that All DoD GIG Components Meet Accreditation Standards

Percentage of DoD Global Information Grid (GIG) Components Accredited


Projected ▨
Percentage of Components Accredited
2nd QTR FY01
4th QTR FY01
2nd QTR FY02
4th QTR FY02